

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Peter J. Mauro, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Kik account that is stored at premises owned, maintained, controlled, or operated by MediaLab.ai Inc. (hereafter Kik), a social networking company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Kik to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Kik account “rclatt” and any Kik account associated with telephone number 330-608-5936 stored at the premises Kik c/o MediaLab.ai Inc.

2. I have been employed as a Special Agent of the FBI since August of 2009 and I am currently assigned to the Cleveland Division, Akron Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the FBI Academy in Quantico, Virginia and everyday work relating to conducting these types of investigations. I am an FBI certified Computer Analysis Response Team (CART) Technician, and an FBI Digital Extraction Technician (DExT). Prior to the FBI, I enlisted in the United States Air Force where I attained the rank of Staff Sergeant. I hold an associate’s degree in criminal justice, a bachelor’s degree in psychology, and a master’s degree in criminal justice.

3. This affidavit is based on my experience and training as well as on information

obtained by me through investigative observations and conversations with other FBI agents, Officers from other state and federal law enforcement agencies, the conversations of a Federal Agent acting in an undercover capacity, the issuance of administrative subpoenas, commercial and government database examinations, social media exploitation, and other authorized investigative means. This affidavit does not set forth every fact resulting from this investigation; rather, it contains a summary of the investigation to date for the limited purpose of establishing probable cause to obtain a search warrant.

4. This investigation concerns alleged violations of Title 18, United States Code, Section 2252, Certain activities relating to material involving the sexual exploitation of minors.

a. Title 18, United States Code, Section 2252(a) prohibits any person who knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails.

DEFINITIONS

5. The following definitions apply to this Affidavit and its Attachments:

a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or

public areas of any person.

c. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

d. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e- mail, remote storage, and co-location of computers and other communications equipment.

e. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers and/or letters separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. A creation IP address is the address used on the date that an e-mail or other account is created by the user.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 United States Code, Sections 2252(a)(2)

have been committed by Raymond Charles Lattimer, utilizing the Kik account “relatt”. There is also probable cause to search the information described in Attachment A for evidence of these crimes, and contraband or fruits of these crimes, as described in Attachment B. I submit this application and affidavit in support of a search warrant authorizing a search of the Kik account “relatt” and any Kik account associated with telephone number 330-608-5936 (hereafter referred to as Subject Kik Account), as further described in Attachments A and B, incorporated herein by reference.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court of the Northern District of Ohio is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND ON KIK

8. Kik is a free service that is downloaded from the Internet. Kik Messenger (aka KIK) advertises itself as “the first smartphone messenger with a built-in browser.” Kik allows users to talk to their friends, browse and share any web site with a Kik user’s friends. According to their website, Kik offers a simple, fast, most life-like chat experience you can get on a smartphone. Unlike other messengers, Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control with whom they communicate. In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, GIFs, sketches, memes, stickers and even more with mobile web pages.

9. The Kik app is available for download for virtually every make and model of modern smartphone via the App Store for most iOS devices such as iPhones and iPads as well as

it is available on the Google Play Store for Android devices. Kik can be used on multiple mobile devices, to include cellular phones and tablets.

10. In general, providers like Kik ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address.

11. Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

12. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems or complaints from other users. Providers typically retain records about such communications, including records of e-mails and other contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

13. As explained below, information stored at MediaLab.ai Inc., parent company of Kik, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation. In my training and experience, the data pertaining to an account that is retained by a provider like Kik can indicate

who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, data collected at the time of account sign-up- and other communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a Kik account at a relevant time. Further, such stored electronic data can show how and when the account was accessed or used. Such “timeline” information allows investigators to understand the chronological context of the usage of an account, account access, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the user of a Kik account. Additionally, stored electronic data may provide relevant insight into the state of mind of the user of a phone number as it relates to the offense under investigation. For example, information relating to a particular Kik account may indicate the user’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

14. Kik offers users the ability to create an identity within the app referred to as a “username”. This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is generally displayed in their Kik profile, and in this case, the username is “Mike Smith”.

15. In October 2019, Kik, formerly headquartered in Canada, was purchased by MediaLab.ai Inc., a company operating in the United States in California.

INVESTIGATIVE DETAILS

16. In or about October 2022, the FBI Cleveland Division, Akron RA was made aware of CyberTip¹ (CT) 135707275 from Synchronoss Technologies Inc² (hereafter referred as “Synchronoss”), concerning one of their users who uploaded Child Sexual Abuse Material (CSAM) by the Ohio Internet Crimes Against Children Task Force (ICAC). In the CT Synchronoss, provided the incident date and time as September 28, 2022, at 21:13:00 UTC, and the subscriber phone number 330-608-5936. Synchronoss also provided one image of CSAM which is described as follows:

- Image titled “6499328bc96b49d4958658c0c10dfc28_1e39ad00db7396f636ef8e324322a1029e2605e3768790063b1aa589704fc4a7.jpg” is a color image which depicts an approximately 6-year-old Caucasian female with blonde hair standing up. The camera is positioned below her body and is pointed up at her. She is wearing pink flower print shorts and a pink flower print top. Her stomach is exposed and her shorts are positioned in such a manner exposing her vulva to the camera.

17. On or about January 11, 2023, a federal search warrant was served on Synchronoss for the cloud account belonging to phone number 330-608-5936. On or about January 13, 2023, an FBI task force officer (TFO) received the production of the contents of that account and began processing and analyzing the information. The TFO conducted a review of

¹ A CyberTip, short for CyberTipline report, is a report submitted to the National Center for Missing and Exploited Children (NCMEC). NCMEC gathers leads and tips regarding suspected online crimes against children and forwards them to the appropriate law enforcement agencies.

² Synchronoss is a cloud-based storage service for Verizon Wireless subscribers and is headquartered in the State of New Jersey.

that production and observed several new CSAM images not previously seen in this investigation. One of the images is described as:

- Image titled “0728D88C-4590-404D-A7E1-01F06B70358A.jpeg” is a color image depicting an approximately six-year-old Caucasian female with red hair wearing only a checkered shirt. Her buttocks is exposed to the camera and she is performing fellatio on an unidentified male’s erect penis. The male is wearing pants which are unzipped and the belt is undone and he appears to be holding a stuffed animal.

18. On or about April 22, 2023, agents of the FBI, as well as your affiant, executed two federal search warrants. One on the person of Lattimer and the other on his residence. Your affiant and a TFO from the FBI conducted an interview with Lattimer. During that interview Lattimer admitted to looking at child pornography for eight to ten years. He said there was currently child pornography on his phone. Lattimer stated he obtained the CSAM from three general online locations; Kik, Wickr³, and an identified adult dating website. Lattimer stated that the Kik account that he uses to receive and view CSAM was “relatt” and that the account was currently logged in on his phone.

19. Lattimer stated he obtained the cellphone containing the CSAM approximately two years before, and identified the phone’s service provider as Verizon Wireless, telephone number, make and model. Lattimer provided the passcode to access the phone. He also demonstrated to me where on the phone CSAM was stored and the applications from where it was derived. The phone account described by Lattimer is the same as the account associated with the Synchronoss search warrant described above.

³ Wickr is a end-to-end encrypted chat application headquartered in New York that is commonly used in the receipt, possession, and distribution of CSAM.

20. Furthermore, Lattimer told your affiant he was communicating with an unidentified female from Australia whom he believed was 13 or 14 years old. Lattimer said this female sent him nude images of herself. When your affiant inquired whether or not he requested the images from this female, he said that it was “mutual”.

21. Lattimer admitted to your affiant that his girlfriend brought her daughter (juvenile #1) over to his house several years ago. Lattimer said that currently juvenile #1 is approximately nine years old. He admitted he has thought about juvenile #1 when masturbating and has thought about touching her but has not acted on those thoughts. Lattimer admitted to your affiant he took photographs of this girl with her pants slightly pulled down exposing her buttocks and has used those photographs while masturbating.

22. Lattimer told your affiant that he looks at child pornography every couple of days, most recently, the day before the encounter with your affiant. Lattimer outlined that he would obtain CSAM from Kik, Wickr and from the identified dating website, then move the CSAM to his phone’s media gallery to save for later use. He also admitted to taking his phone containing CSAM with him across state lines and looking at child pornography on his device while he is out of state for work in his hotel room. Lattimer stated that he is specifically aroused by talking to teens about when they first start masturbating.

23. Lattimer was confronted with a folder of printed color images of small, clothed children age approximately three to six years old photographed in innocuous circumstances. Lattimer stated that the images depicted his grandchildren. Lattimer denied any hands-on offenses with the children but stated that he avoids contact with them because he is worried that he will be tempted by their presence.

24. Lattimer was provided his cellular telephone, which I had a federal search warrant to search. Lattimer volunteered the areas of his phone that contained CSAM, including Kik. Lattimer showed me and a TFO his Kik account, including where it was logged in to the account “rclatt”.

25. Lattimer later provided a signed-written statement regarding his conduct to another FBI Agent. In that statement, Lattimer admitted to asking for or receiving nude images or sexual depictions of minors between 100 and 200 times while chatting online. He admitted that the Australian female mentioned above sent him images and photographs depicting her engaged in sex acts. The two communicated for about a year and a half. Later in that same statement, Lattimer admitted that his girlfriend brought juvenile #1 to his residence. Lattimer again admitted to photographing juvenile #1 with her pants down and viewing those photographs in a sexual manner. Lattimer further stated that he expressed to his girlfriend that he would only have sexual contact with juvenile #1 under the right circumstances in which he knew no one would get hurt and everyone was consenting to the sexual activity.

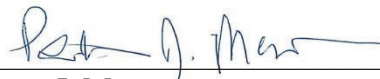
26. On or about April 22, 2023 I served a preservation request to Kik for account “rclatt”.

CONCLUSION

27. Based on the forgoing, I hereby file this Application for an order requiring Kik, a premises owned, maintained, controlled, or operated by MediaLab.ai Inc., an electronic communications service provider, to provide contents of electronic communications and electronic files pertaining to the Kik account “rclatt” and any Kik account associated with cellular telephone number 330-608-5936, and request that the Court issue the proposed search warrant authorizing the search of the account described in Attachment A for the items described

in Attachment B.

28. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on MediaLab.ai Inc. Because the warrant will be served on MediaLab.ai Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.



Peter J. Mauro
Special Agent
Federal Bureau of Investigation

Sworn to via telephone after submission by
reliable electronic means. Crim. Rules 4.1;
41(d)(3) this 25th day of April, 2023.



AMANDA M. KNAPP
UNITED STATES MAGISTRATE JUDGE